Annual Report to Congress on Foreign nomic Collection dustrial Espiona

1995

JULY 1995

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage

1995

JULY 1995

Contents

Jul 95

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage

Introduction

Section 809 of the *Intelligence Authorization Act for Fiscal Year 1995* required that the President report to the Congress on foreign industrial espionage targeted against US industry. The Act defined foreign industrial espionage as "industrial espionage conducted by a foreign government or by a foreign company with direct assistance of a foreign government against a private United States company and aimed at obtaining commercial secrets." The *Act* required that the report address four issues:

a. The respective policy functions and operational roles of the agencies of the Executive Branch of the Federal Government in identifying and countering threats to US industry of foreign industrial espionage, including the manner in which such functions and roles are coordinated.

b. The means by which the Federal Government communicates information on such threats, and on methods to protect against such threats, to US industry in general and to US companies known to be targets of foreign espionage.

c. The specific measures that are being or could be undertaken in order to improve the activities referred to in the above paragraphs, including proposals for any modifications of law necessary to facilitate the undertaking of such activities.

d. The threat to US industry of foreign industrial espionage and any trends in that threat, including:

1. The number and identity of the foreign governments conducting foreign industrial espionage.

2. The industrial sectors and types of information and technology targeted by such espionage.

3. The methods used to conduct such espionage.

The National Counterintelligence Policy Board (NACIPB), on behalf of the National Security Council, tasked the National Counterintelligence Center (NACIC) to draft a community-based response to this Congressional requirement. The NACIC solicited input from the relevant Executive Branch agencies, including the Federal Bureau of Investigation (FBI), National Security Division; the Central Intelligence Agency (CIA), Counterintelligence Center; the Department of State, Bureaus of Intelligence and Research and Diplomatic Security; the Director of Counterintelligence and Security Programs in the Office of the Assistant Secretary of Defense for Command, Control, Communication, and Intelligence; the Defense Intelligence Agency (DIA); the US Army Intelligence and Security Command; the Naval Criminal Investigative Service (NCIS); the Air Force Office of Special Investigations (OSI); the Defense Investigative Service (DIS); the Personnel Security Research Institute; the National Security Agency (NSA); the Department of Energy (DOE), Counterintelligence Division; the Department of Commerce, Office of Export Enforcement; the Department of Treasury, Office of Intelligence Support; and the US Customs Service, Office of Intelligence. Input from each of these agencies has been incorporated into this report.

This study describes the "defensive" measures that the US Government applies to counter foreign collection of US economic-related intelligence and information. It also lists the US targets of foreign economic collection and the methods foreign governments and corporations use to obtain US economic and technological information, including at times US Government information that directly affects US industry. This study does not address the concept of the US Government "offensively" collecting foreign proprietary information and providing it to US firms, which is against US policy.

To provide a full scope of foreign economic collection efforts targeted at US firms, this report examines "foreign industrial espionage" as specifically requested by Congress as well as other types of collection efforts that potentially could be damaging to US national and corporate interests. This report includes collection efforts by foreign intelligence services, other government agencies, and private firms, in two broad classes of economic collection activities—espionage and illicit acquisition of proprietary information, and other economic collection efforts. In distinguishing between different types of collection activity, this report is not designed to establish legal parameters for the activities described, nor to characterize the actions and decisions of US law enforcement and intelligence agencies with regard to counterintelligence (CI) operations and investigations.

Espionage and Illicit Acquisition of Proprietary Information. Espionage and illicit collection activities represent attempts by foreign governments and/or industry to acquire classified or nonpublic information from US firms. Government-sponsored activities are conducted by entities such as intelligence services, other government agencies—such as foreign trade offices and S&T attaches—and private corporations.

Other Economic Collection Efforts. Foreign governments and industry also collect economic information from US firms through standard business practices—such as mergers and acquisitions,[1] strategic alliances, and licensing agreements—as well as gathering publicly available information. Although these activities are an accepted element of the business world and are largely peripheral to the scope of this report, a large body of reporting indicates that these activities generate a considerable portion of the technology and economic information obtained by our competitors. They clearly do not constitute illegal behavior, however. Open-source collection activities include, but are not limited to, review of trade journals or corporate annual reports, market surveys, and attending conferences and symposia. In some instances, however, these types of collection efforts could be precursors to illicit collection activities or indicate the intelligence interest of foreign powers. For example, attempts by a foreign government's intelligence service to persuade an employee of a US firm to gather information from the firm's library could be the first step in setting up a source that would eventually collect proprietary documents. Similarly, joint ventures and licensing agreements provide ideal opportunities to gather nonpublic information from US firms.

This report is divided into four sections, corresponding with the four parts of the Congressional requirement. A classified version of this report accompanies this document.

[1] The US Government has procedures to review foreign purchases of US firms to determine if the acquisition is likely to have an adverse effect on US national security interests. Mergers and acquisitions with firms having classified US Government contracts are governed by the National Industrial Security Program, established by Executive Order 12829, which provides security safeguards for classified information at contractors under foreign ownership, control, or influence. In addition, the Committee on Foreign Investment in the United States (CFIUS) reviews—under statutory procedures—various foreign mergers and acquisitions of US firms to determine the impact on US national security.

I. Policy Functions and Operational Roles

Report the respective policy functions and operational roles of the agencies of the Executive Branch of the Federal Government in identifying and countering threats to US industry of foreign industrial espionage, including the manner in which such functions and roles are coordinated.

The US Government's primary methods for identifying and countering foreign economic espionage and illicit acquisition of proprietary information are CI operations and law enforcement investigations. CI and law enforcement agencies monitor foreign intelligence collection, ascertain how and against whom it is directed, and determine the optimum remedy to counter the threat, either through CI methods or criminal prosecution.

CI efforts are directed at monitoring, penetrating, and neutralizing foreign intelligence activities targeted against US national interests, including economic and industrial interests. Law enforcement agencies take advantage of CI information as well as develop their own information through investigations. At times, these two communities have proceeded separately without effectively coordinating their efforts. Section III of this study contains several Executive Branch options to ensure better coordination and cooperation.

The FBI is the central US Government agency for collecting, analyzing, and investigating foreign threats to US industry. Because of its mission as both the US Government's primary CI agency with regard to foreign intelligence activities within the United States and in its role as the lead criminal investigative agency, the FBI is able to use both types of remedies against economic and industrial espionage. The FBI recently created two new investigative classifications—one for cases in which there is alleged or confirmed foreign power involvement and one for purely criminal cases—to better counter the problem. Current internal FBI administrative reform is designed to optimize the use of CI and law enforcement remedies.

The US Customs Service is the US Government's primary border enforcement agency with responsibility for enforcing several categories of laws that relate to illegal economic activities. For example, Customs is responsible for enforcing the Arms Export Control Act and the Export of War Materials Act, which involve munitions control and trafficking activities. It is also responsible for the enforcement of export controls of high-technology material and information under the Export Administrations Act. Economic and industrial espionage are often connected to trade sanctions and embargoes against designated countries, strategic trade issues, and protection of intellectual property rights, and thus fall under Customs responsibilities.

Each Department of Defense (DOD) military service has CI and criminal investigative components that conduct CI operations and investigate foreign economic and industrial intelligence activities as they relate to DOD programs and systems. Military services work closely with the FBI when the activity involves violations of Federal laws or intelligence activity targeted against US persons. The information developed through this support is disseminated and coordinated throughout the CI and security programs communities.

CI and law enforcement investigative agencies rely on several sources within the US Government for CI information and criminal leads that they further develop through investigations and operations, including the following:

- The FBI's Development of Espionage, Counterintelligence, and Counterterrorism Awareness (DECA) Program provides an interface with the US corporate community through which the FBI not only conveys information but also obtains investigative leads from

corporations concerning foreign government and corporate attempts to illicitly collect US economic and technological information.

- The CIA informs the FBI and other appropriate US Government agencies when it learns, in the course of its broader foreign CI and economic intelligence-gathering activities, about a foreign government or company targeting US industry. For example, the CIA informs the FBI and/or the Department of Justice of economic espionage information acquired from foreign government sources. In addition, the CIA informs the State Department and other appropriate government agencies of instances of economic espionage or state-supported unfair trading practices, such as bribery of contracting officials. The CIA also prepares analysis on countries engaging in economic espionage and questionable trading practices for dissemination to US Government policymakers and throughout the Intelligence Community.

- DOE's Counterintelligence Division manages a defensive CI program to identify and counter threats of foreign economic and industrial intelligence collection activities against DOE personnel and facilities. DOE collects information through reports on foreigners visiting DOE facilities and through debriefings of DOE employees and contractors who may have been targeted by foreign governments or corporations. It furnishes this information as CI leads to the FBI when there is evidence of foreign intelligence targeting.

- DIS systematically collects CI information developed through personnel security interviews and industrial security inspections. The Counterintelligence Office analyzes this information and, when appropriate, provides it as CI and criminal investigative leads to agencies such as the FBI, US Customs Service, and the military services.

II. US Government Support to Private Industry

Report the means by which the Federal Government communicates information on [industrial espionage] threats, and on methods to protect against such threats, to US industry in general and to US companies known to be targets of foreign espionage.

US Government agencies identify and counter foreign economic espionage and illicit efforts to acquire proprietary information from two distinct but integrated approaches: CI and law enforcement. As a subset of those approaches, and taking advantage of the information that the respective communities develop, the US Government also counters those activities through awareness training.

Awareness programs are designed to provide government and private audiences with the foreign threat information they need to better protect classified and proprietary economic information from illicit collection. US Government contractors receive the vast majority of threat information that flows from government to industry. Recipients include contractors for the National Aeronautics and Space Administration (NASA), CIA, and the Departments of Defense, Energy, and State.

The primary US Government programs that pass threat information to non-government affiliated corporations are the FBI's DECA Program; the State Department's Overseas Security Advisory Council (OSAC); and, on occasion, the CIA's National Resources Division. NACIC, which recently completed a survey of the CI needs of US industry, also has implemented initiatives to work with these various programs to provide more timely or relevant threat information to the private sector.

After obtaining information indicating that a specific US company is being targeted by a foreign intelligence service or government, the US Intelligence Community (USIC) shares it with the FBI which may inform the US company about the threat. The FBI may brief appropriate personnel in the company about the threat and work with them to counteract that threat. Information of a more general nature also is shared with the State Department's OSAC representatives for passage to the private sector. The NACIC will join forces with OSAC to share threat information, particularly on the US technology targeted and collection techniques used by foreign governments.

The following tabulation lists the awareness and briefing programs within each US Government agency that provides threat information to private-sector companies:

USG Agency	Recipient of CI and Threat Information
CIA	Selected US persons and companies
DIA	DOD contractors
DIS	DOD contractors
DOD/ASPP	DOD contractors and defense acquisition community
DODSI	Briefings and *Security Awareness Bulletin* to numerous industry customers
Military Services	Contractors working on service R&D programs, special access programs, and military systems acquisition programs
DOE	DOE contractors, CRADA participants
FBI	All US industry
NACIC	Selected US industry
NASA	NASA contractors
NSA	NSA contractors
USDS/DS/OSAC	Member companies

Federal Bureau of Investigation

The DECA Program is the FBI's public voice and educational medium for communicating foreign threat information, especially the economic espionage threat, to the private sector. The DECA Program has

been in place for over 20 years and has been an integral part of the FBI's foreign CI program. DECA coordinators in each of the FBI's 56 field offices have regular liaison with companies located in the field offices' territories. The DECA coordinators furnish briefings, videotapes, pamphlets, and other materials to help the private sector understand and recognize foreign economic espionage threats directed at them. The content of briefings and material provided is tailored to the specific needs and concerns of each company. The DECA coordinators also discuss the various methods employed by foreign governments to accomplish their intelligence collection goals. During fiscal years 1993 and 1994, the FBI briefed almost 20,000 companies totaling nearly a quarter of a million personnel, in addition to briefings at academic institutions, laboratories, and state and local governments.

The DECA Program is a national effort with management, direction, and analytical support from FBI Headquarters. As needed, FBIHQ provides field offices with information, materials, and speaker support to facilitate a specific request or need. It relies on dynamic and direct communication between the DECA coordinator and executives, security directors, and personnel in US corporations. In addition, the program periodically publishes a foreign intelligence threat information journal titled *DECA Notes*. Both classified and unclassified versions of *DECA Notes* and DECA briefings have been given to US corporations throughout the United States.

Department of State

State Department's OSAC is a joint venture by the Department and US businesses to interact on overseas security problems of mutual concern, including foreign economic threats. OSAC is administered under the State Department's Bureau of Diplomatic Security (DS). Over 1,400 private-sector organizations participate in its activities and receive information and guidance. As part of the growing emphasis on the threat to US business, OSAC established a Committee for Protection of Information and Technology that seeks to improve the government-industry partnership.

OSAC also oversees "Country Councils" in selected foreign cities that consist of US embassy security officers and other post officials working with security managers of US private-sector enterprises to exchange unclassified security information in a timely fashion. There are Country Councils in 25 foreign cities, with five more planned for 1995. Country Councils enable OSAC to pass threat information to industry and to gather information from US corporations concerning threats to US economic security.

Government and business representatives have joined with OSAC to produce a series of publications providing guidance, suggestions, and planning techniques on a variety of security-related issues, including a booklet titled *Guidelines for Protecting US Business Information Overseas*, the latest version of which was published in November 1994.

To exchange threat information as expeditiously as possible, the State Department created the OSAC Electronic Bulletin Board (EBB). The EBB is an unclassified on-line system available to OSAC member companies that serves as the focal point for the exchange of information between the Department of State and the US private sector. More specifically, DS's Office of Intelligence and Threat Analysis (ITA) uses the EBB to provide US corporations doing business abroad with timely, unclassified security-related information. US firms supplement ITA's information by voluntarily submitting accounts of security or crime incidents affecting their own or other US overseas operations. The EBB currently contains over 42,000 individual reports of various types of threats overseas.

Central Intelligence Agency

The CIA provides information to the FBI for use, as appropriate and in accordance with memoranda of understanding and executive orders, in the DECA Program. On occasion, the CIA briefs US corporate officials directly concerning the foreign intelligence threats facing US companies. The CIA has presented

these briefings, which describe the ways various countries conduct economic intelligence collection against the United States, to individual corporations and at industry-wide conferences, often with FBI participation. The briefings cover foreign economic activities worldwide, focusing on intelligence-gathering techniques used by specific countries. The CIA plans to offer another briefing on commercially available technical gear used by foreign services to conduct economic espionage against US companies.

As appropriate, CIA coordinates with other US Government agencies, specifically the FBI, before notifying a US company that it is the specific target. CIA also is participating extensively in planning and implementing an array of activities under the auspices of the NACIC's new interagency Awareness Working Group (see below). These programs are designed to inform and assist US companies that are actual or potential targets.

Department of Defense

The ***Defense Intelligence Agency***, under its Defense Information Counter Espionage (DICE) program, conducts briefings at conferences attended by government-affiliated contractors and provides current threat information for training courses for DOD contractor personnel. The subjects of these briefings include economic intelligence collection activities by friendly countries and threats of illicit technology transfer. DIA also prepares CI risk assessments on foreign ownership of DOD-affiliated US corporations and studies on the foreign intelligence threat to DOD programs and operations, including contractor programs.

The ***Defense Investigative Service*** shares information with industry about targeting of specific technologies or specific contractors based on its analysis of information from data bases such as the Foreign Ownership, Control, or Influence (FOCI) data base and various elements of the Foreign Disclosure and Technical Information System. The focus of the DIS program is to safeguard classified information, but its efforts also help to protect proprietary information. As DIS becomes aware of the targeting of specific technologies or specific contractors, that information is shared with industry and other US Government agencies as appropriate.

Foreign threat information also is developed by DIS Special Agents during personal security interviews (PSIs), by Industrial Security representatives under the auspices of the National Industrial Security Program, and through liaison with other US agencies. Reports are disseminated throughout DOD, throughout the USIC, and to cleared defense contractors during industrial security actions.

DIS is developing a program to identify cleared facilities that are involved in critical technologies and have interface with foreign interests. They will spearhead a briefing/debriefing program for contractor personnel who host foreign national visitors, conduct foreign travel/visits, interface with on-site foreign national visitor groups, and are assigned overseas. The focus of this program will be to identify attempts by foreign nationals to circumvent or undermine disclosure decisions.

DOD Service CI Components each have comprehensive programs to brief the defense industry and the acquisition community on the political, military, and economic threat to sensitive technologies and programs and the multidisciplinary threat posed by foreign countries, visitors, and economic entities. Military CI components provide a full range of CI support to the military research, development, test, and evaluations community; acquisition program offices; and contractors they serve. Their overall goal is to detect, deter, neutralize, and exploit attempts by foreign entities to acquire restricted DOD systems and technologies.

The ***DOD Acquisition Systems Protection Program (ASPP)*** attempts to unify the acquisition, CI, and security communities to prevent losses of information. Under ASPP, the acquisition community identifies the most essential elements of DOD acquisition programs, known as EPITS (essential program information, technology, and systems), as well as other pertinent information about DOD technologies. The CI community identifies threats to the technologies

in general and to specific EPITS by location as far as possible. The security community then tailors countermeasures to offset the threat and vulnerabilities of the program.

The ***Department of Defense Security Institute (DODSI)*** develops and presents courses of instruction in DOD Security Countermeasures programs, including industrial, personnel, information, and security awareness and management programs. Discussions of the threat are inherent in these programs. DODSI also publishes unclassified security awareness information. The most well-known DODSI publication is the *Security Awareness Bulletin*, which is distributed to over 25,000 customers in government and industry and provides an easy vehicle for disseminating CI information. Articles often highlight foreign economic and industrial intelligence activities and ways to protect against them. DODSI is in the process of producing a series of security awareness videos titled *Countering Espionage*.

National Reconnaissance Office

NRO's Counterintelligence Staff runs a CI threat and awareness program to brief its contractor-based personnel on the intelligence threat targeting their systems and programs.

National Security Agency

The NSA conducts briefings and develops and organizes courses, seminars, and conferences to sensitize its contractors cleared for special compartmented information to the foreign intelligence threat domestically and overseas. NSA provides general and country-specific threat information in all indoctrination and orientation briefings, debriefings, and special briefings (for example, defensive travel briefings, courier briefings, special access briefings, and so forth).

NSA products are not provided directly to the private sector, and there are currently no plans to do so. On rare occasions when specific threat information of import to a US company is developed by NSA, the information may be provided to the FBI. Subject to NSA approval, a "sanitized" FBI threat notification may be made to the firm.

National Counterintelligence Center

The NACIC was established in 1994 in accordance with Presidential Decision Directive/NSC-24, titled "US Counterintelligence Effectiveness." It is the NACIPB's primary mechanism to guide all national-level CI activities, including countering foreign economic and industrial intelligence collection activities.

The NACIC Threat Assessment Office has begun to compile intelligence and open-source reporting on the clandestine targeting of US industry and technologies by foreign powers or their intelligence services. It fulfills this in cooperation with other US Government agencies in three ways:

1. By providing analyses on threats to emerging or existing technologies and on threats to critical facilities in the United States or overseas.

2. By identifying and broadly disseminating information on human and technical collection methods used by foreign powers against the United States, including threats encountered by US businessmen at home or overseas.

3. By assessing the CI aspects of foreign disclosures, foreign ownership, technology transfers, and joint ventures.

In cooperation with other US Government agencies, the NACIC has begun to provide certain reports, as appropriate based upon classification and dissemination caveats, to US private firms with and without classified government contracts. The NACIC has responded to limited taskings from US corporations for threat information and will seek to make this service more available to private-sector customers.

The NACIC Program Integration Office, through the NACIC Awareness Working Group, also serves as a community coordinating body for CI training and awareness programs. As such, it facilitates the development and monitors the effectiveness of US Government awareness programs for both the public and private sectors. CI information describing the threat to US industry is incorporated into these awareness presentations.

The NACIC is currently participating in two surveys of private industry. The first was conducted in coordination with OSAC, under the direction of the National Security Council. It was distributed in December 1994 and January 1995 to OSAC member companies. This survey was designed to identify ways to enhance the relationship between the CI community and US private industry. It sought the opinion of industry on how the US Government could better provide private corporations with information on the threat from foreign intelligence and security services overseas and in the United States. Results of this survey are now being tabulated and will be used to help formulate US Government policy on how to best fill the CI needs of US industry. The NACIC is also participating in a spring 1995 survey, in conjunction with the American Society of Information Security (ASIS) and Michigan State University, to gauge the severity of the theft of proprietary information in the private sector. This survey is designed to update and validate a 1992 ASIS survey on the same subject. The survey will be distributed to approximately 6,000 US corporations, and results are planned to be published by summer 1995.

Department of Energy

DOE's CI Program mission is to deter and neutralize foreign intelligence activities in the United States directed at or involving DOE programs, facilities, technology, personnel, and sensitive unclassified and classified information. The DOE Counterintelligence Division communicates the foreign threat through its awareness training program, analysis program, foreign travel briefing and debriefing programs, and the dissemination of foreign intelligence threat information to employees, scientists, managers, and security personnel. The Counterintelligence Division regularly publishes classified and unclassified analytical studies, bulletins, newsletters, and other information about foreign intelligence threats to DOE facilities and personnel. This threat information is also shared with other US Government agencies and US corporations who have entered into cooperative research and development agreements (CRADAs) with DOE.

Department of Commerce

Although the Department of Commerce does not have a formal program to provide CI support to US business, it provides informal assistance through security awareness briefings to contractors and consultants with access to classified information. Its Office of Export Enforcement conducts an industry outreach program that provides information to numerous industry officials each year on CI as it relates to illegal technology transfer. Various Department of Commerce components also publish newsletters and magazines that contain highlights of security incidents and illicit export practices.

US Customs Service

In support of its multifaceted mission, Customs has for years operated several education and outreach programs designed to familiarize private industry with the export laws and regulations and with the Customs Service roles in enforcing them. These programs have included threat information when it applies to export issues.

National Aeronautics and Space Administration

NASA provides specific threat information to NASA employees and contractors involved in Special Access Programs through approximately 1,500 security awareness briefings annually. Although there are no NASA resources solely dedicated to conducting awareness briefings, security specialists are usually assigned the task.

III. Options for Consideration

Report the specific measures that are being or could be undertaken in order to improve the activities referred to in the above paragraphs, including proposals for any modifications of law necessary to facilitate the undertaking of such activities.

CI efforts are governed by presidential directives, executive orders, and statutes, many of which were established during the Cold War and were designed to counter a corresponding threat: that is, foreign intelligence activities directed against US military and political information. Over the past three years, some of these guidelines have been adapted to better confront the post–Cold War reality that economic and technological information are as much a target of foreign intelligence collection as military and political information.

Law enforcement efforts are similarly limited because economic and technological information is often not specifically protected by Federal laws, making it difficult to prosecute thefts of proprietary technology or intellectual property. Law enforcement efforts instead must rely on less specific criminal laws—such as espionage, fraud and stolen property, and export statutes—to build prosecutable cases against foreign economic and industrial intelligence collectors and to deter such activity. The Administration is considering legislative options to strengthen current Federal statutes, and possibly to establish new laws that would specifically forbid theft of intellectual property and proprietary information.

While other options are under various stages of consideration, the following are included as examples:

Executive Branch Policy Options

Increase resources available to US CI and law enforcement organizations to investigate and, where appropriate, prosecute entities involved in industrial and economic intelligence collection activities targeting US information.

As attested by the Aldrich Ames espionage case, the end of the Cold War has not stopped traditionally hostile foreign intelligence services from collecting information via espionage. US CI agencies continue to allocate resources against traditional intelligence threats. However, while such threats have continued, an increasing portion of US CI and law enforcement resources is also being drawn to thwart economic and industrial intelligence collection activities. Some of these more recently identified activities are conducted by traditional threat countries and can be investigated with existing resources directed against those countries.

Countries that heretofore have not been considered intelligence threats account for much of the economic collection currently being investigated by the US CI and law enforcement communities. Since the CI community does not have the benefit of years of accumulated experience investigating such efforts, these investigations are often labor intensive. Resources in these areas will likely have to be increased, especially if the theft of proprietary

information is made a Federal violation, since the result would be an increased number of cases requiring more trained investigators and analysts.

Institutionalize the concept that economic security is an integral part of national security.

The goal of US CI is to identify, penetrate, and neutralize foreign intelligence activities that threaten US national security. CI has traditionally been directed at military, ideological, or subversive threats to national security. Until the past several years, countering activities that threaten economic security had not usually been included.

In today's world in which a country's power and stature are often measured by its economic/industrial capability, foreign government ministries—such as those dealing with finance and trade—and major industrial sectors are increasingly looked upon to play a more prominent role in their respective country's collection efforts. While a military rival steals documents for a state-of-the-art weapon or defense system, an economic competitor steals a US company's proprietary business information or government trade strategies. Just as a foreign country's defense establishment is the main recipient of US defense-related information, foreign companies and commercially oriented government ministries are the main beneficiaries of US economic information. The aggregate losses that can mount as a result of such efforts can reach billions of dollars per year, constituting a serious national security concern.

The March 1990 and February 1995 national security strategies published by the White House focus on economic security as an integral part not only of US national interest but also of national security.

In February 1995, President William J. Clinton published *A National Security Strategy of Engagement and Enlargement* in accordance with the Goldwater-Nichols Defense Department Reorganization Act of 1986. It identified the US central goals as:

- To sustain our security with military forces that are ready to fight.
- To bolster America's economic revitalization.
- To promote democracy abroad.

The report identifies US intelligence capabilities as critical instruments of national power and notes:

> *The collection and analysis of intelligence related to economic development will play an increasingly important role in helping policy makers understand economic trends. That collection and analysis can help level the economic playing field by identifying threats to US companies from foreign intelligence services and unfair trading practices. (p.17)*

The report describes the US Government partnership with business and labor, noting:

> *Our economic strategy views the private sector as the engine of economic growth. It sees government's role as a partner to the private sector—acting as an advocate of US business interests; leveling the playing field in international markets; helping to boost American exports; and finding ways to remove domestic and foreign barriers to the creativity, initiative and productivity of American business. (p.19)*

Guidance issued from 1990 to the present directs the Intelligence Community and CI community specifically to detect and deter foreign intelligence targeting of US economic and technological interests, including efforts to obtain US proprietary information from companies and research institutions that form our strategic industrial base.

Consistent with US national security policy since 1990, then, the CI community should emphasize economic security in operations, reports, and briefings designed to fulfill the guidance outlined above.

Develop a coordinated CI and law enforcement approach and appropriate collection and analytic requirements to address foreign economic and industrial intelligence collection activities.

Previous reports sponsored by the Executive and Legislative Branches have found that efforts across the government to investigate and counter economic and industrial intelligence collection activities were often fragmented and uncoordinated. The CI and law enforcement communities have usually not effectively harmonized their efforts. Numerous interagency working groups and committees had been formed to discuss the problem, while at the same time a number of individual agencies were exerting their own efforts. This lack of coordination resulted in many partially informed decisions and diverging collection and analytical efforts. The Executive Branch is developing a coordinated CI and law enforcement approach and appropriate collection and analytic requirements.

Since its inception, the NACIC has made efforts to determine the CI needs of various traditional and nontraditional intelligence consumers. In the process of surveying agency customers, the NACIC discovered that many needs have not fully been met in the past, either because no mechanism was in place to fulfill the needs or because the existing mechanism was malfunctioning. As part of the NACIC's program of determining CI needs, it will assist in forming appropriate and manageable requirements to ensure that 1) necessary information is being collected and 2) once the information is collected, it reaches those that need it.

Systematically collect and analyze information about the efforts of foreign countries not traditionally considered intelligence threats, along with corporations from those countries, to collect protected US Government and corporate information.

Over the past several months, the NACIC has interviewed over 170 officials from 62 US Government agencies—both those that are customarily involved in CI and those who have not usually been included in such efforts—to determine the CI needs of the US Government. Several policymakers interviewed cited a lack of information on the activities of countries that have not traditionally been considered intelligence threats but that may be mounting aggressive intelligence targeting efforts against our leading-edge technologies, economic infrastructure, and personnel. They desire better information about whether information and technology shared with allies through legitimate projects are being siphoned off and provided to foreign competitors, and how much information is being acquired by foreign students studying at US universities and research centers. They are also interested in what intelligence capabilities the US Government is providing to friendly foreign countries through liaison relationships that could be used to collect US information. More proactive and aggressive collection against intelligence services and corporate information collection personnel from countries traditionally allied with the United States is needed to fill these intelligence gaps.

IV. Foreign Economic Threat

Report on the threat to US industry of foreign industrial espionage and any trends in that threat, including:

1. The number and identity of the foreign governments conducting any but foreign industrial espionage.

A. Country Case Studies

A number of foreign countries pose various levels and types of threats to US economic and technological information. Some have been considered ideological and military adversaries for decades. Their targeting of US economic and technological information is not new but has continued as an extension of a concerted intelligence assault on the United States conducted throughout the Cold War. Others are either longtime allies of the United States or have traditionally been neutral. These countries target US economic and technological information despite their friendly relations with the United States. In some cases, they take advantage of their considerable legitimate access to US information and collect sensitive information more easily than our military adversaries. In addition, some of the countries traditionally considered allies have infrastructures that allow them to easily internalize high-tech information and utilize it in competition against US firms.

The evidence indicating which countries and corporations conduct economic and industrial espionage against the United States is derived from numerous classified and open sources. Because of the ramifications to US foreign policy as well as the sensitivity of source information, the specific identities of countries are included in the classified report only.

2. The industrial sectors and types of information and technology targeted by such espionage.

B. Targeted Information and Technology

The industries that have been the targets in most cases of economic espionage and other collection activities include biotechnology; aerospace; telecommunications, including the technology to build the "information superhighway"; computer software/hardware; advanced transportation and engine technology; advanced materials and coatings, including "stealth" technologies; energy research; defense and armaments technology; manufacturing processes; and semiconductors. Proprietary business information—that is, bid, contract, customer, and strategy—in these sectors is aggressively targeted. Foreign collectors have also shown great interest in government and corporate financial and trade data.

These industries are of strategic interest to the United States because they produce classified products for the government, produce dual use technology used in both the public and private sectors, and are responsible for leading-edge technologies critical to maintaining US economic security. Many other US high-tech industrial sectors have been targeted. Any company competing for a sale or a piece of market share, regardless of the market, could resort to intelligence activities as a "force multiplier" to improve its chances of success.

Currently, there is no formal mechanism for determining the full qualitative and quantitative scope and impact of the loss of this targeted information. Industry victims have reported the loss of hundreds of millions of dollars, lost jobs, and lost market share. However, these reports have been ad hoc and often only after public exposure of the loss. Understandably, US industry is reluctant to publicize occurrences of foreign economic and industrial espionage. Such publicity can adversely affect stock values, customers' confidence, and ultimately competitiveness and market share.

3. The methods used to conduct such espionage.[2]

C. Collection Methods

Practitioners seldom use one method in isolation but combine them into concerted collection programs. Although countries or corporations have been known to turn legitimate transactions or business relationships into clandestine collection opportunities, some of the methods listed are most often used for legitimate purposes. While their inclusion here is not intended to imply illegal activity, they are listed as potential elements of a broader, coordinated intelligence effort.

Traditional Methods
Traditional espionage methods primarily reserved for collecting national defense information are now being applied to collect economic and proprietary information. Traditional awareness training is most suitable for countering these collection methods.

Classic Agent Recruitment. An intelligence collector's best source is a trusted person inside a company or organization whom the collector can task to provide proprietary or classified information. A foreign collector's interest in employees is not necessarily commensurate with their rank in the company. Researchers, key business managers, and corporate executives can all be targets, but so can support employees such as secretaries, computer operators, technicians, and maintenance people. The latter frequently have good, if not the best, access to competitive information. In addition, their lower pay and rank may provide fertile ground for manipulation by an intelligence agency.

US Volunteers. The individuals most likely to improperly acquire a company's information are the company's own employees. Employees who resort to stealing information exhibit the same motivations and human frailties as the average thief or spy: illegal or excessive use of drugs or alcohol, money problems, personal stress, and just plain greed.

Surveillance and Surreptitious Entry. Economic and industrial espionage may involve simply breaking into an office containing desired information. Companies have reported break-ins in which laptop computers or disks were stolen, even when there were easily obtainable, more valuable items in the same vicinity. These instances are not always reported, or reported as merely break-ins, without considering the possibility that the target was information rather than equipment.

Some countries convince hotel operators to provide intelligence collectors with access to visitors' luggage or rooms. During these surreptitious break-ins, known colloquially as "bag ops," unattended luggage is searched for sensitive information, and any useful documents are copied or simply stolen.

Specialized Technical Operations. This includes computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses. These activities account for the largest portion of economic and industrial information lost by US corporations.

[2] These descriptions are adapted from a 1993 interagency study on foreign intelligence threats to US economic interests.

Because they are so easily accessed and intercepted, corporate telecommunications—particularly international telecommunications—provide a highly vulnerable and lucrative source for anyone interested in obtaining trade secrets or competitive information. Because of the increased usage of these links for bulk computer data transmission and electronic mail, intelligence collectors find telecommunications intercepts cost-effective. For example, foreign intelligence collectors intercept facsimile transmissions through government-owned telephone companies, and the stakes are large—approximately half of all overseas telecommunications are facsimile transmissions. Innovative "hackers" connected to computers containing competitive information evade the controls and access companies' information. In addition, many American companies have begun using electronic data interchange, a system of transferring corporate bidding, invoice, and pricing data electronically overseas. Many foreign government and corporate intelligence collectors find this information invaluable.

Economic Disinformation. Some governments also use disinformation campaigns to scare their domestic companies and potential clients away from dealing with US companies. Press and government agencies frequently discuss foreign economic and industrial intelligence activities, often in vague, nonspecific terms. The issue has been used to paint foreign competitors or countries as aggressive and untrustworthy, even if the accuser has no tangible evidence of any collection activity. Some countries have widely publicized their efforts to set up information security mechanisms to protect against their competitors' penetration attempts, and frequently the United States is mentioned as the primary threat.

Other Economic Collection Methods

Tasking Foreign Students Studying in the United States. Some foreign governments task foreign students specifically to acquire information on a variety of economic and technical subjects. In some instances, countries recruit students before they come to the United States to study and task them to send any technological information they acquire back to their home country. Others are approached after arriving and are recruited or pressured based upon a sense of loyalty or fear for their home country's government or intelligence service.

In some instances, at a intelligence collector's behest, foreign graduate students serve as assistants at no cost to professors doing research in a targeted field. The student then has access to the professor's research and learns the applications of the technology.

As an alternative to compulsory military service, one foreign government has an organized program to send interns abroad, often with the specific task of collecting foreign business and technological information.

Tasking Foreign Employees of US Firms and Agencies. Foreign companies and governments sometimes recruit or task compatriot employees within a US firm to steal proprietary information. Although similar to clandestine recruitment used traditionally by intelligence services, often no intelligence service is involved, only a competing company or nonintelligence government agency. The collector then passes the information directly to a foreign firm or the government for use in its R&D activities.

Debriefing of Foreign Visitors to the United States. Some countries actively debrief their citizens after foreign travel, asking for any information acquired during their trips abroad. Sometimes these debriefing sessions are heavyhanded, with some foreign scientists describing them as offensive. In other countries, they are simply an accepted part of traveling abroad.

Recruitment of Emigres, Ethnic Targeting. Frequently, intelligence collectors find it effective to target persons of their own ethnic group. They particularly seek individuals working in US military and R&D facilities who have access to proprietary and classified US technology. Several countries have

found repatriation of emigre and foreign ethnic scientists to be the most beneficial technology transfer methodology. One country, in particular, claims to have repatriated thousands of ethnic scientists back to their home country from the United States. Ethnic targeting includes attempts to recruit and task naturalized US citizens and permanent resident aliens to assist in acquiring US S&T information. Frequently, foreign intelligence collectors appeal to a person's patriotism and ethnic loyalty. Some countries' collectors resort to threatening family members that continue to reside in their home country.

Elicitation During International Conferences and Trade Fairs. Events—such as international conferences on high-tech topics, trade fairs, and air shows—attract many foreign scientists and engineers, providing foreign intelligence collectors with a concentrated group of specialists on a certain topic. Collectors target these individuals while they are abroad to gather any information the scientists or engineers may possess. Sometimes, depending on the foreign country and the specific circumstances, these elicitation efforts are heavyhanded and threatening, while other times they are subtle.

Foreign intelligence collectors sometimes attempt to recruit scientists by inviting them on expense-paid trips abroad for conferences or sabbaticals. The individuals are treated royally, and their advice is sought on areas of interest. When they return to the United States, collectors recontact them and ask them to provide information on their areas of research.

Commercial Data Bases, Trade and Scientific Journals, Computer Bulletin Boards, Openly Available US Government Data, Corporate Publications. Many collectors take advantage of the vast amount of competitive information that is legally and openly available in the United States. Open-source information can provide personality profile data, data on new R&D and planned products, new manufacturing techniques, and competitors' strengths and weaknesses. Most collectors use this information for its own worth in their business competition. However, some use openly available information as leads to refine and focus their clandestine collection and to identify individuals and organizations that possess desired information.

Clandestine Collection of Open-Source Materials. Because they believe that they are closely monitored by US CI, some traditional intelligence services resort to clandestine methods to collect even open-source materials. They have been known to use false names when accessing open-source data bases and at times ask that a legal and open relationship be kept confidential.

Foreign Government Use of Private-Sector Organizations, Front Companies, and Joint Ventures. Some foreign governments exploit existing non-government affiliated organizations or create new ones—such as friendship societies, international exchange organizations, import-export companies, and other entities that have frequent contact with foreigners—to gather intelligence and to station intelligence collectors. They conceal government involvement in these organizations and present them as purely private entities in order to cover their intelligence operations. These organizations spot and assess potential foreign intelligence recruits with whom they have contact. Such organizations also lobby US Government officials to change policies the foreign government considers unfavorable.

Corporate Mergers and Acquisitions. Several countries use corporate mergers and acquisitions to acquire technology. The vast majority of these transactions are made for completely legitimate purposes. However, sometimes they are made specifically to allow a foreign company to acquire US-origin technologies without spending their own resources on R&D.

According to a 1994 US Government report, entitled *Report on US Critical Technology Companies*, 984 foreign mergers and acquisitions of US critical technology companies occurred between 1 January 1985 and 1 October 1993. All but a handful of these mergers and acquisitions were friendly, and four countries